

Application No. 09/996,283
Amendment dated September 23, 2005
Reply to Office Action of March 23, 2005

REMARKS

Claims 1-23 are pending and under consideration. The remarks following the paragraph numbering of the office action.

Rejection of Claim 1 Under 35 U.S.C. § 112, Second Paragraph

The Examiner has rejected claim 1 because the recitation of "active agent" on line 12 lacks antecedent basis. Applicant has amended line 12 of claim 1 to recite "second active agent."

Rejection of Claims 1-3, 5, 7, 9-12, 14, 16, and 18-23 Under 35 U.S.C. § 102(e) as Allegedly Anticipated by US 6,351,536 ("Sasaki")

Claims 1-3, 5, 7, 9-12, 14, 16, and 18-23 stand rejected as allegedly anticipated by US 6,351,536 ("Sasaki"). Applicant respectfully disagrees.

Sasaki requires the creation of public/private key pairs for all users and acknowledges that the use of public/private key pairs increases administrative overhead and security risks (*see* column 1, lines 27-33). The presently claimed invention provides significant innovation over the cited reference because it does not require the creation of public/private key pairs for all users. Thus, the presently claimed invention provides an encryption method that reduces administrative overhead and security vulnerabilities (*see* ¶0005 of the instant specification).

¶¶4-11. Sasaki discloses two major components, the "transmitter" and the "receiver," connected via a network (*see* FIG 1). Sasaki does not disclose the "key management component" of the presently claimed invention, *i.e.*, the cited reference does not disclose a "key management component" that is distinct from a "transmitter" or "receiver." Unlike Sasaki, the presently claimed invention's "key management component" is the only element in the invention that performs the operation of public/private key generation (*see* step 500, FIGS 4 & 5). In contrast to Sasaki, the presently claimed invention only needs to create one public/private key pair, which further reduces administrative overhead and security vulnerabilities when compared to the cited reference.

Both the presently claimed invention and the cited reference recite the step of first encrypting data with a symmetric key and then encrypting the symmetric key with a public key.

Application No. 09/996,283
Amendment dated September 23, 2005
Reply to Office Action of March 23, 2005

This is an industry standard method of encryption "Public-Key Cryptography Standard (PKCS) #7 Cryptographic Message Syntax Standard" (*see* <http://www.rsasecurity.com/rsa/labs/node.asp?id=2129>).

In the method of the presently claimed invention, the sender encrypts the clear text with a symmetric key (*see* step 1210, FIG 8 of the specification) and then encrypts the symmetric key with the key management component's public key (*see* step 1220, FIG 8).

In the method of Sasaki, the sender, "transmitter", also encrypts the clear text with a symmetric key, "common key" (*see* step 102, FIG 5). However, the sender then encrypts the symmetric key (step 105) with a public key that was generated by the receiver (step 201). Figures 4-8, 10, 12-14, 16, 18, 20-22 all show the receiver generating public/private key pairs that are uniquely associated with that receiver. This follows the practice of PKCS #7, identified above.

The "server" of the cited reference (*see* FIGS 19-22) does not correspond to the presently claimed invention's "key management component." This is because the inclusion of the "server" does not eliminate the requirement for "receivers" to generate public/private key pairs (*see* col. 22, lines 62 - 67).

¶12. Sasaki does not teach the method of claim 10 because it does not teach a "key management component." Specifically, Sasaki decrypts the symmetric key with the recipient's private key, not the key management component's private key, because again, the Sasaki does not teach a "key management component."

¶13. Sasaki does not teach the methods of claims 2 and 19 because it does not teach a "key management component" nor does it teach the encryption program recited by claim 2 and 19. Sasaki generates a public/private key pair for an individual recipient, not for the overall method as recited in claims 2 and 19. Because Sasaki teaches encryption programs that require public/private key pairs, it does not teach the encryption programs recited in claims 2 and 19.

¶14. Sasaki does not teach the method of claims 11 and 12 or the system of claim 21 because it does not teach a "key management component" nor does it teach decryption of the symmetric

Application No. 09/996,283
Amendment dated September 23, 2005
Reply to Office Action of March 23, 2005

key with the system's (key management component's) private key as recited by claims 11, 12 and 21. Sasaki teaches decrypting the symmetric key with the recipient's private key.

¶15. Sasaki does not teach the system of claim 22 because it does not teach a "key management component" nor does it teach the server recited by claim 22. The Examiner cited to col. 13, lines 55-57 of Sasaki as teaching "under control of a client system, requesting a clear text object from a server" Applicant respectfully points out that col. 13, lines 55-57 refers to sending cipher text from the transmitter to the receiver.

¶16. Sasaki does not teach the system of claims 20 and 23 because it does not teach a "key management component" nor does it teach public/private key pairs for the system as recited by claims 20 and 23. Sasaki teaches public/private key pairs for individual recipients.

For these reasons, it is respectfully submitted that Sasaki does not disclose the "key management component" of independent claims 1, 10, 19, 20, 21, 22, and 23. Additional bases of rejection asserted against claims depending from claim 1 or claim 10 are moot in view of the distinctions of claims 1 and 10. Based on the foregoing, Applicant requests withdrawal of the rejection.

Rejection of Claims 4, 6, 8, 13, 15, and 17 Under 35 U.S.C. § 103(a) as Allegedly Unpatentable Over US 6,351,536 ("Sasaki")

Claims 4, 6, 8, 13, 15, and 17 stand rejected as unpatentable over US 6,351,536 ("Sasaki"). Applicant respectfully disagrees.

¶¶18-21. The prior art references when combined must teach or suggest all of the claim limitations. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). It follows that when the combination is based on a subset of elements selected from the cited references, all of the claim elements must be present in the cited references. Here, as discussed above, Sasaki does not teach the "key management component" of the presently claimed invention and thus does not teach the method of claims 1 and 10. The knowledge of one of skill in the art cited by the

Application No. 09/996,283
Amendment dated September 23, 2005
Reply to Office Action of March 23, 2005

Examiner does not make up for the deficiencies of Sasaki. Based on the foregoing, Applicant request withdrawal of the rejection.

Double Patenting

¶¶25-29. Claims 1-23 are rejected under the doctrine of nonstatutory double patenting over claims 1-30 of copending US Application No. 09/735,875. Applicant respectfully points out that US Application No. 09/735,875, entitled "Implosion Prevention Band for a CRT" issued as US Patent 6,488,166. Applicant suspects the Examiner meant to cite US Application No. 09/735,876, not US Application No. 09/735,875. US Application No. 09/735,876 went abandoned February 2, 2005. Thus, the rejection is moot.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Rosemarie L. Celli
Registration No. 42,397

SUGHRUE MION, PLLC
Telephone: (650) 625-8100
Facsimile: (650) 625-8110

MOUNTAIN VIEW OFFICE

23493

CUSTOMER NUMBER

Date: September 23, 2005

32378v1